IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 5, April 2024

Reinforcing Cybersecurity with GAN-Enabled Intrusion Detection

Smt. BH D D Priyanka[1], N Srujana[2], K Sai Lakshmi[3], K Leela Padmavathi[4], M Geetha Vani[5]

Assistant Professor, Department of Information Technology[1]

Students, Department of Information Technology[2,3,4,5]

S.R.K.R Engineering College, Bhimavaram, Andhra Pradesh, India

namburisrujana1992@gmail.com

Abstract*: In the realm of cybersecurity, Intrusion Detection Systems (IDS) are essential tools for identifying network attacks. While traditional machine learning algorithms have been widely used in security, they've struggled to keep pace with evolving technology and the challenges of modern cyber threats. This has led to a gradual decline in the effectiveness of machine learning-based intrusion detection systems. However, there's hope on the horizon in the form of Generative Adversarial Networks (GANs). GANs have garnered attention for their ability to effectively detect anomalies in complex, high-dimensional data. By leveraging deep learning techniques, we can address the shortcomings of traditional machine learning algorithms in intrusion detection. This study proposes to explore the use of GANs and their variations for network intrusion detection using real-world datasets. The aim is to demonstrate the feasibility of this approach and provide comparative results to evaluate its effectiveness.*

Keywords: cybersecurity

I. INTRODUCTION

1. Background

As network and information technology continue to evolve and become increasingly prevalent in our daily lives, the digital realm has become deeply intertwined with various aspects of society. With individuals, organizations, and governments storing critical and confidential data online, the importance of cybersecurity has grown exponentially. Among the key defense mechanisms in cybersecurity is Intrusion Detection Systems (IDS), which analyze sample data distributions to identify unauthorized activities that may compromise the confidentiality, integrity, or availability of information. Traditional machine learning algorithms have been extensively employed to enhance IDS efficiency due to their flexibility and effectiveness. However, the rise in the complexity and volume of malicious attacks has magnified certain limitations of traditional machine learning methods, such as their focus on processing low-dimensional data and the manual selection of features.

In recent years, there has been a rapid advancement in the application of deep learning algorithms, such as Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and Automatic Encoder (AE), in intrusion detection. Additionally, Generative Adversarial Networks (GANs), a class of deep learning algorithms introduced by Goodfellow et al. in 2014, have demonstrated significant potential in generating high-dimensional data and improving anomaly detection performance across various domains. GANs offer several advantages in intrusion detection, including their ability to mimic any data distribution and their effectiveness against adversarial attacks.

Despite these advantages, research on the utilization of GANs in intrusion detection remains limited, presenting an opportunity for further exploration and investigation.

2. Intrusion Detection Systems

In the domain of cybersecurity, Intrusion Detection Systems (IDS) stand as vital pillars, offering frontline defense for computer systems and networks against a wide spectrum of threats. Their core function involves actively monitoring network traffic and scrutinizing data generated by individual host devices. Operating under the fundamental tenet of "Monitor-Detect-Respond," IDS are essential for swiftly identifying and addressing any suspicious activity.

DOI: 10.48175/IJARSCT-17513

They are broadly classified into two main categories: Host-based IDS, focusing on safeguarding individual devices, and Network-based IDS, which oversee overall network traffic. Intrusions, marked by unauthorized access or misuse of computer systems by both internal and external actors, highlight the urgent necessity for robust IDS solutions. By promptly identifying and countering hostile attacks, IDS play a pivotal role in safeguarding industries worldwide, ensuring the integrity and security of digital infrastructures.

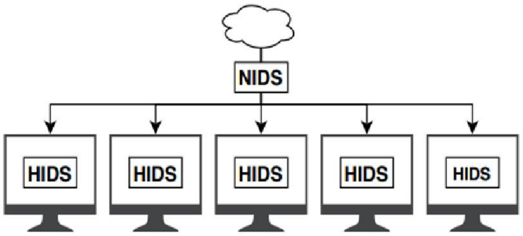


Fig. 1. IDS Types

2.1. Host-based IDS

A host-based intrusion detection system (HIDS) primarily operates within individual computers, nodes, or devices. While its core function is internal monitoring, various HIDS variants also facilitate network monitoring. HIDS detect system compromises by scrutinizing the entire communication stream, alerting administrators to suspicious activities such as rogue program access or harmful registry modifications.

2.2. Network-based IDS

Network-based intrusion detection systems (NIDS) are designed to monitor and analyze network traffic, playing a crucial role in safeguarding systems against network-based threats. Their primary function is to detect unauthorized malicious access to a Local Area Network (LAN) and examine traffic traversing across wires and multiple hosts. Detection algorithms scrutinize both inbound and outbound packets for any suspicious patterns, triggering alerts to notify administrators. NIDS technology encompasses three different network topologies, including direct connection to switches, spanning ports using network taps, and inline connections. These systems provide a blend of traditional IT security measures and specific measures tailored to the unique features of Industrial Control Systems (ICS).

The architecture of a generic NIDS comprises several key components:

- Data gathering sensors: These sensors monitor the infrastructure where data gathering occurs, observing specific processes or protocols and performing primary data classification based on the received data.
- Detector engine: This module compares the gathered data against defined rule sets. When the IDS detects a deviation from the normal status, it raises an alarm.
- Storage Module:This component houses the rule sets of the IDS, which the detector utilizes when comparing received data.
- Response: Upon triggering an alarm, the IDS responds with a precisely defined action. Depending on the type of alarm, this response could involve performing a predefined action such as dropping malicious packets or adopting a passive response such as logging the activity for human decision-making.

Real-time Intrusion Detection:

Intrusion detection systems can be developed for offline or real-time detection. Offline detection involves working with long-term data, aggregating information about individual clients or behavior patterns over time. While effective, this mechanism can be time-consuming for certain system designs. Conversely, real-time intrusion detection aims to identify intrusions as they occur or shortly thereafter, ensuring timely responses to continuously incoming data streams.

3. Generative Adversarial Networks

Generative Adversarial Networks (GANs) operate on a min-max strategy, pitting two algorithms against each other: one acting as the generator and the other as the discriminator. The generator's aim is to produce data, while the

DOI: 10.48175/IJARSCT-17513

discriminator's role is to differentiate between fake and real data. The generator strives to maximize the discriminator's error, while the discriminator endeavors to minimize it. This iterative process continues until the discriminator's error reaches 0.5, indicating a 50% failure rate, which serves as the baseline error in bi-classification.
Conceptually, a GAN can be likened to a "Cat and Mouse Game" between a detective and a counterfeiter, where the counterfeiter (generator) attempts to deceive the detective (discriminator), perpetuating an ongoing cycle of improvement through competition. To generate synthetic data, the generator relies on a source of creativity, typically derived from a random noise vector (seed). Conversely, to discern between real and fake data, the discriminator requires access to a database of authentic images.

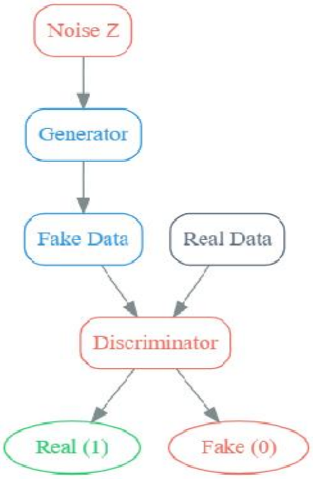


Fig. 2. Generative Adversarial Network.

4. Standardization

Within the domain of Intrusion Detection Systems (IDS), standardization emerges as a pivotal preliminary measure in handling heterogeneous data streams, encompassing logs of network traffic and system-generated records. Through standardization, each feature is transformed to attain an average of 0 and a standard deviation of 1, thus ensuring that all features contribute uniformly to the detection model, irrespective of their original scale or unit of measurement. This equalization of feature importance enhances the model's capability to discern nuanced patterns and anomalies indicative of security breaches, thereby bolstering the system's ability to proactively identify and respond to cyber threats.

5. Scope

This research aims to evaluate IDS models based on GANs by varying parameters to assess their performance. The study will involve collecting theoretical research data on GANs and implementing IDS based on these models, followed byrunning simulations and evaluating the results using metrics such as confusion matrices.

6. Objectives of the project

- Develop a GAN-based Intrusion Detection System (IDS) to enhance anomaly detection accuracy in network traffic.
- Train the GAN model to generate realistic network traffic patterns, enabling effective differentiation between normal and malicious activities.
- Evaluate and optimize the GAN-based IDS to improve detection rates while minimizing false positives, thereby strengthening overall network security.

DOI: 10.48175/IJARSCT-17513

II. LITERATURE SURVEY (RELATED WORK)

1. Early Detection of OS Scan Attacks in Intrusion Detection Systems (IDS)
Author: Manuel López-Vizcaíno
Published: 2019
Description:
Network Intrusion Detection Systems (NIDS) aim to identify unauthorized access to computer networks by analyzing traffic to detect malicious activity. Rapid detection of intrusions is crucial to disrupt the Cyber Kill Chain effectively. While conventional evaluations rely on accuracy metrics like precision or F-measure, they often overlook detection time. This paper introduces the concept of early intrusion detection and evaluates existing time-aware metrics, proposing a new metric called NormERDE. Results highlight that high precision may not necessarily translate to swift threat detection, underscoring the importance of time-aware metrics in NIDS evaluations for real-world effectiveness.

2. Enhancing IDS Performance through Early Detection in Local Area Networks Using Industrial Control Systems of Honeypots
Author: Abbasgholi Pashaei
Published: 2020
Description:
The security of Industrial Control Systems (ICS) in cybersecurity networks is critical to ensuring operational continuity and safeguarding against threats. This study introduces an Industrialized Early Intrusion Detection System (EIDS) by modifying traditional Intrusion Detection System (IDS) methods. Leveraging routers, IDS Snort, Industrial honeypots, and Iptables MikroTik, EIDS effectively simulates and implements instructions for intrusion detection, displaying attacker information on a dedicated monitoring page tailored for ICS environments.

3. Intrusion Detection and Attack Classification Using Feed-Forward Neural Networks
Author: Fariba Haddadi
Published: 2010
Description:
This paper addresses the importance of Intrusion Detection Systems (IDSs) in network security, focusing on a 2-layered feed-forward neural network approach. It employs an "early stopping" strategy during training to mitigate overfitting issues. The proposed IDS is evaluated using DARPA dataset, demonstrating notable performance improvements through preprocessing and feature range conversion. The simplicity and effectiveness of the system underscore its suitability for robust intrusion detection.

4. Evaluation of Machine Learning Techniques for Network Intrusion Detection
Author: Marzia Zaman
Published: 2018
Description:
Anomaly detection plays a crucial role in network security by identifying potential intrusions. This study evaluates seven machine learning techniques with information entropy calculation for anomaly detection, using the Kyoto 2006+ dataset. Results indicate high precision, recall, and accuracy across most techniques, with the Radial Basis Function (RBF) performing notably well based on the area under the Receiver Operating Curve (ROC) metric.

5. Intrusion Detection System in Smart Home Networks Using Artificial Immune System and Extreme Learning Machine Hybrid Approach
Author: Yang Xu
Published: 2020
Description:
The proliferation of Internet of Things (IoT) devices in smart homes introduces security vulnerabilities. This paper presents an early work on an Intrusion Detection System (IDS) for smart home networks, employing Extreme Learning

Machine and Artificial Immune System (AIS-ELM). AIS optimizes input parameters using the clonal Algorithm, while ELM analyzes parameters for enhanced anomaly detection. The IDS, designed for integration with smart home gateways, aims to detect and notify homeowners of network anomalies for timely action.

III. METHODOLOGY

This section elaborates on the complexities of the proposed framework for the intrusion detection system (IDS) as illustrated in Figure 3.

The innovative methodology introduced for Intrusion Detection Systems (IDS) signifies a groundbreaking departure from traditional cybersecurity paradigms, offering a fresh perspective to tackle inherent challenges. Unlike conventional machine learning-based techniques, which often grapple with the complexity and multi-dimensional nature of real-world network data distributions, the proposed methodology leverages Generative Adversarial Networks (GANs) to surmount these obstacles. At its core, the methodology embraces adversarial learning through GAN architecture, enabling the effective comprehension of intricate data distributions. This pioneering approach empowers the IDS to discern subtle patterns and behaviors inherent in network traffic data, thereby facilitating more precise and resilient anomaly detection.

The methodology commences with an exhaustive Data Preprocessing phase, where stringent protocols are implemented to ensure the quality and integrity of the data. This entails meticulous cleaning, normalization, and handling of missing values, establishing a robust foundation for subsequent analysis. Following this, the Feature Extraction module identifies and selects pertinent features crucial for constructing a coherent dataset, enabling the IDS to concentrate on the most pertinent aspects of network traffic. However, the crux of the methodology lies in the GAN module, where an adversarial training process unfolds. Here,a Generator and Discriminator engage in a dynamic interplay, with the Generator tasked with generating synthetic yet realistic network traffic data, while the Discriminator endeavors to differentiate between authentic and synthetic instances. This adversarial learning mechanism enables continuous learning and adaptation to the complexities of real-world network data, thereby significantly enhancing the IDS's anomaly detection capabilities. Additionally, the methodology underscores the significance of ongoing evaluation and optimization.

Here's a breakdown of the methodology into steps:

1. Data Preprocessing:

- The initial step involves preparing raw network data for analysis, encompassing:
- Cleansing: Eliminating errors, inconsistencies, or irrelevant data.
- Normalization: Ensuring consistent format and scale for further processing.
- Handling Missing Values: Addressing gaps or missing information to prevent biases.

2. Feature Extraction:

- Once the data is organized, relevant features are extracted, involving:
- Identification: Determining pertinent aspects like packet size and communication patterns.
- Selection: Choosing key features to differentiate normal from malicious behavior.

3. Generative Adversarial Networks (GANs) Module:

Generative Adversarial Networks (GANs) mark a groundbreaking advancement in artificial intelligence, harnessing adversarial learning to produce synthetic data that faithfully mirrors real-world distributions. In our project, GANs play a pivotal role in bolstering the capabilities of the Intrusion Detection System (IDS) by generating synthetic network traffic data. This enhancement addresses a core challenge in cybersecurity by enriching training datasets, thereby amplifying the diversity and volume of data accessible for robust pattern recognition and anomaly detection. Unlike conventional methodologies, GANs excel in capturing the complex and multidimensional distributions inherent in network traffic data, transcending the limitations of traditional approaches.

In the IDS framework, GANs function through the deployment of a generator and a discriminator engaged in a dynamic adversarial interplay, participating in a minimax game where the generator strives to produce synthetic data closely

DOI: 10.48175/IJARSCT-17513

resembling genuine network traffic, while the discriminator's aim is to effectively differentiate between authentic and synthetic instances. Through the utilization of synthetic data, the IDS bolsters its resilience against adversarial attacks and evasion tactics employed by sophisticated adversaries. The incorporation of GANs facilitates ongoing learning and refinement, ensuring the IDS remains adaptable and efficient in identifying evolving threats within intricate network environments. In summary, the integration of GANs empowers the IDS to uphold network integrity, enhancing cybersecurity posture and resilience against the continually evolving landscape of cyber threats.

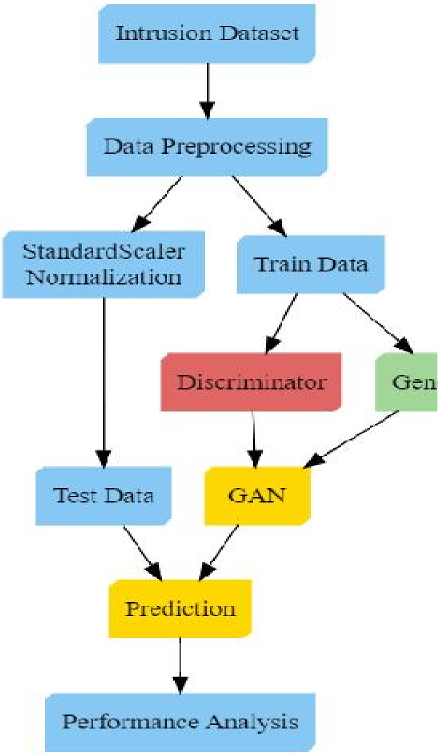


Fig. 3. Proposed Methodology.

Generator:

Within our project, the generator component of the Generative Adversarial Network (GAN) architecture holds a pivotal role in synthesizing realistic network traffic data, essential for training the Intrusion Detection System (IDS). By leveraging randomly generated noise vectors as input and transforming them into data samples closely resembling genuine network traffic patterns, the generator facilitates the IDS in learning from a diverse and representative dataset. This process of generating synthetic data is crucial for addressing the challenge of constrained and imbalanced training datasets commonly encountered in cybersecurity applications. Through the augmentation of the training dataset with synthetic samples, the IDS can more effectively capture the intricate and dynamic nature of network traffic, thereby enhancing its capacity to detect and classify anomalous behavior with heightened accuracy and robustness. Furthermore, the generator's ability to produce realistic synthetic data enables adaptive learning within the IDS, empowering it to dynamically adapt and evolve in response to emerging cybersecurity threats and evolving network environments. In essence, the generator's role in synthesizing data is pivotal in empowering the IDS to achieve heightened levels of accuracy, efficiency, and adaptability in safeguarding network integrity and countering malicious activities, thereby bolstering overall cybersecurity posture and resilience.

Discriminator:

In our project, the discriminator in the Generative Adversarial Network (GAN) architecture acts as the crucial judge, distinguishing between real network traffic and artificially generated samples. Through an adversarial learning process, it refines its ability to identify subtle patterns and anomalies in network data, driving the generator to produce more convincing fake data. This improvement cycle enhances theoverall performance of our Intrusion Detection System (IDS) by providing more accurate and realistic data for analysis. Moreover, the discriminator's role extends beyond training the GAN; it also evaluates incoming network traffic during the detection phase, ensuring our system remains adaptive and effective in addressing evolving cybersecurity challenges.

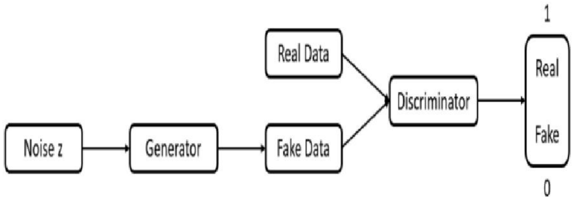


Fig. 4. Generator And Discriminator.

Adversarial Training:

Adversarial training is a core technique used in deploying Generative Adversarial Networks (GANs) within the project. This method involves training two neural networks: the generator (referred to as G) and the discriminator (denoted as D), in a competitive manner. The goal is to improve the generator's ability to produce synthetic data resembling real data, while the discriminator aims to accurately distinguish between authentic and synthesized data. This adversarial learning process continues iteratively until an equilibrium is reached, where the generator generates data challenging for the discriminator to differentiate. When D's output stabilizes around 0.5, it indicates that G has successfully learned to generate synthetic data distributions closely resembling the actual data distribution. At this equilibrium, neither G nor D can further enhance their performance, signifying successful adversarial training. This process enables GANs to effectively generate high-fidelity synthetic data.

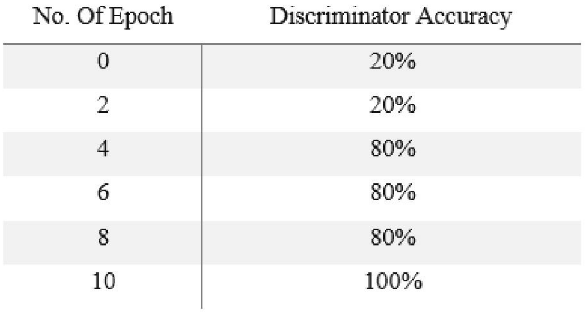
The dataset is divided into separate sets for learning and evaluation, allocating 80% of the data for learning and 20% for evaluation. This split ensures sufficient data for model training while reserving a distinct portion for performance assessment. Additionally, the formula:

$$\min\max V(D,G) = E_{x\sim p_{\text{data}}(x)}[\log D(x)] +$$

$$E_{z\sim p_z(z)}\left[1 - \log D\big(G(z)\big)\right] \quad (1)$$

represents the objective function of the adversarial training process in GANs. This formula is integral to the minimax game played between the discriminator (D) and the generator (G). In this two-player game, the generator aims to produce data samples resembling original data, while the discriminator strives to accurately differentiate between genuine and synthesized data samples. Specifically, Ex∼pdata (x) [log D(x)] represents the anticipated score of the discriminator's output when processing genuine data samples (x) from the actual data distribution (pdata (x)). The discriminator aims to maximize this expression, accurately classifying real data samples as authentic. Similarly, the expression Ez ∼ p(z)[1−logD(G(z))] represents the expected logarithmic score of the discriminator's output when presented with synthetic data samples (G(z)) generated by the generator from random noise (z) drawn from a noise distribution (p(z)). The generator aims to minimize this component, producing artificial data examples perceived as authentic by the discriminator.

Table 1 Discriminator with number of Epoch



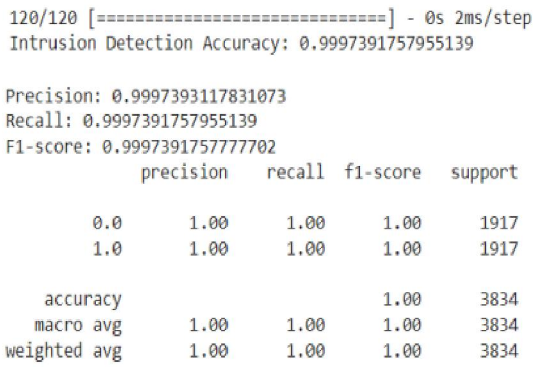
No. Of Epoch	Discriminator Accuracy
0	20%
2	20%
4	80%
6	80%
8	80%
10	100%

Anomaly Detection:
Employing both real and synthetic data, the next step involves employing techniques for anomaly detection, utilizing advanced algorithms to differentiate between normal and malicious behaviors and leveraging synthetic data alongside real data to train the anomaly detection model.

Continuous Evaluation and Optimization:
The final phase focuses on continuous monitoring and refinement of the IDS, ensuring its effectiveness over time by:
Regularly assessing IDS performance using metrics and benchmarks.
Optimizing the system based on performance feedback to adapt to evolving cyber threats and improve resilience.
Ensuring IDS adaptability to quickly respond to new threats and maintain effectiveness in protecting the network.
Overall, this methodology utilizes GANs to create a robust IDS, enhancing network security by effectively detecting and mitigating emerging cyber threats. By integrating comprehensive data preprocessing, feature extraction, GAN-based synthetic data generation, anomaly detection, and continuous evaluation, the IDS remains adaptable and resilient in the face of evolving cybersecurity challenges.

IV. RESULT

Examining Intrusion Detection with Generative Adversarial Networks (GANs) reveals an intriguing pattern in the discriminator's accuracy across multiple epochs. Initially, during GAN model training, the discriminator exhibits high accuracy in distinguishing between genuine and synthesized data, marking the early phase of the process where the generator produces easily identifiable fake data. However, as training progresses, the discriminator's accuracy gradually decreases, indicating the generator's advancement in generating more realistic data that challenges the discriminator's ability to classify. This decrease in discriminator accuracy indicates the success of the adversarial training process, where the generator and discriminator continuously compete and evolve to improve the authenticity of generated data. Ultimately, this observed trend suggests promising results for intrusion detection using GANs.



```
120/120 [==============================] - 0s 2ms/step
Intrusion Detection Accuracy: 0.9997391757955139

Precision: 0.9997393117831073
Recall: 0.9997391757955139
F1-score: 0.9997391757777702
              precision    recall  f1-score   support

         0.0       1.00      1.00      1.00      1917
         1.0       1.00      1.00      1.00      1917

    accuracy                           1.00      3834
   macro avg       1.00      1.00      1.00      3834
weighted avg       1.00      1.00      1.00      3834
```

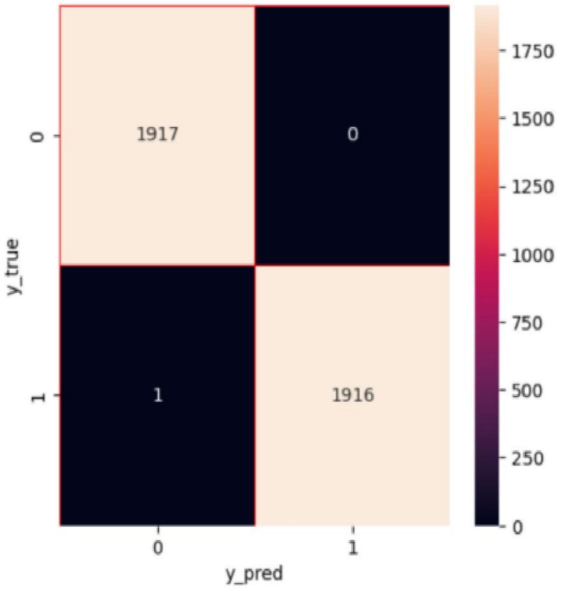
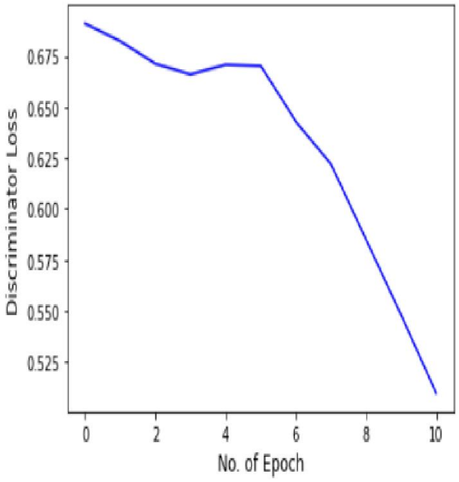


Fig. 5. Confusion Matrix



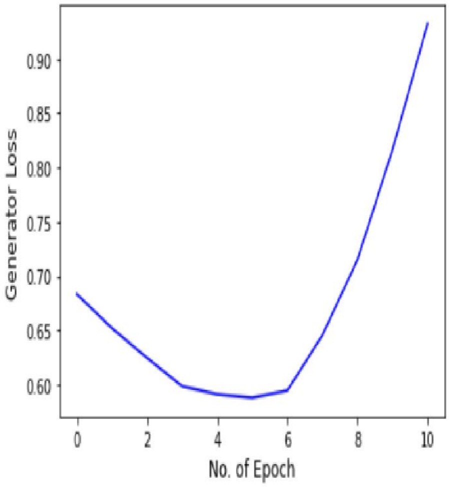


Fig. 6. Discriminator Loss

Fig. 7. Generator Loss

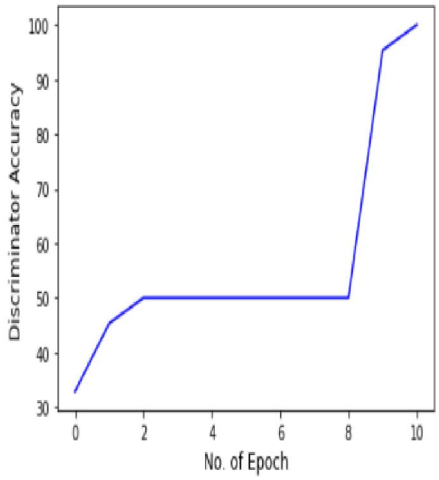


Fig. 8. Discriminator Accuracy

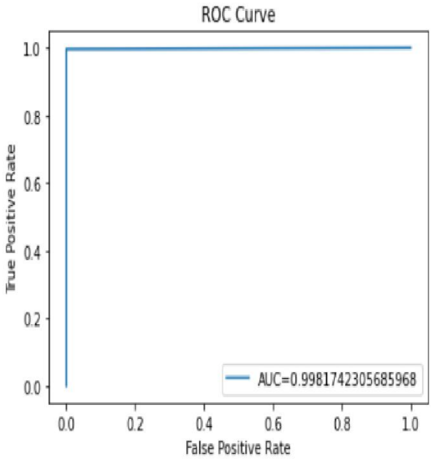


Fig. 9. ROC Curve

V. FUTURE WORK

Future endeavors in advancing the intrusion detection system with GANs entail delving into sophisticated GAN architectures and training methodologies to refine the generation of authentic network traffic data. Furthermore, incorporating reinforcement learning techniques for adaptive model adjustments in real-world scenarios could enhance system efficacy. Exploring the scalability of GAN-based IDS to accommodate extensive and varied datasets, along with extending the approach to integrate multi-modal data sources, presents promising avenues for future exploration. These efforts aim to ensure resilient and efficient intrusion detection capabilities amidst evolving cybersecurity challenges.

VI. CONCLUSION

In conclusion, the integration of Generative Adversarial Networks (GANs) into an Intrusion Detection System (IDS) presents a state-of-the-art approach to strengthening network security. By leveraging GANs, the system generates synthetic yet authentic network traffic data, enhancing the detection of anomalies and potential intrusions with greater accuracy and adaptability. Through meticulous data preprocessing and feature extraction, the IDS is equipped with a robust set of relevant features for comprehensive analysis. At the heart of the system, the GAN module facilitates adversarial training between a generator and discriminator, bolstering the model's ability to discern normal from malicious network activities.

The anomaly detection module enables proactive defense against emerging cyber threats by identifying deviations from expected behavior. Continuous evaluation, optimization, and adaptation mechanisms further bolster the system's resilience. In essence, the IDS powered by GANs serves as a sophisticated and dynamic defense mechanism, fortifying network infrastructures against the constantly evolving landscape of cybersecurity challenges.

Obtaining an AUC (Area Under the Curve) value of 0.999739 represents outstanding performance, highlighting the model's ability to accurately distinguish between positive and negative cases. The confusion matrix (Fig. 5) provides insight into the classification performance, revealing 1917 true negatives (TN), 0 false positives (FP), 1 false negatives (FN), and 1916 true positives (TP). The impressive AUC value of 0.999 on the ROC curve underscores the model's precision, as evidenced by the steep ascent indicative of high true positive rates while maintaining low false positive rates. Leveraging GANs for generating realistic synthetic data during training confers advantages in adaptability and effectiveness in combating cybersecurity threats.

REFERENCES

[1]. Al-Yaseen, Wathiq & Idrees, Ali, MuDeLA: multi-level deep learning approach for intrusion detection systems. International Journal of Computers and Applications,1-9,2023, http://dx.doi.org/10.1080/1206212X.2023.2275084

[2]. Note, Johan & Ali, Maaruf. Comparative Analysis of Intrusion Detection System Using Machine Learning and Deep Learning Algorithms. Annals of Emerging Technologies in Computing. 6. 19-36, 2022, http://dx.doi.org/10.33166/AETiC.2022.03.003 .

[3]. a K, Meeradevi&Sunagar, Pramod &Kanavalli, Anita. (2022). Intrusion Detection System Using Deep Learning. http://dx.doi.org/10.4018/978-1-7998-8161-2.ch009 .

[4]. P. Shettar, A. V. Kachavimath, M. M. Mulla, N. D. G and G. Hanchinmani, "Intrusion Detection System using MLP and Chaotic Neural Networks," International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-4, https://doi.org/10.1109/ICCCI50826.2021.9457024

[5]. B. Budler and R. Ajoodha, "Comparative Analysis of Deep Learning Models for Network Intrusion Detection Systems," 2022 IEEE 2nd Conference on Information Technology and Data Science (CITDS), Debrecen, Hungary, 2022, pp. 45-50, http://dx.doi.org/10.1109/CITDS54976.2022.9914128 .

[6]. Mohammadpour, L.; Ling, T.C.; Liew, C.S.; Aryanfar, A. A Survey of CNN-Based Network Intrusion Detection. Appl. Sci. 2022, 12, 8162. https://doi.org/10.3390/app12168162 .

[7]. Lansky, Jan & Ali, Saqib & Mohammadi, Mokhtar & Majeed, Mohammed & Karim, Sarkhel& Rashidi, Shima & Hosseinzadeh, Mehdi & Rahmani, Amir. Deep Learning-Based Intrusion Detection Systems: A Systematic Review. IEEE Access, 2021, http://dx.doi.org/101574-101599. 10.1109/ACCESS.2021.3097247

[8]. Supriya Shende, Samrat Thorat, 2020, Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security, International Journal of Engineering Research & Technology (IJERT) Volume 09, 2020, https://doi.org/10.17577/IJERTV9IS061016 .

[9]. Altaha, Mustafa & Lee, Jae-Myeong & Muhammad, Aslam & Hong, Sugwon, Network Intrusion Detection based on Deep Neural Networks for the SCADA system. Journal of Physics: Conference Series.1585.012038,2020, http://dx.doi.org/10.1088/1742-6596/1585/1/012038 .

[10]. H. Yang, L. Cheng and M. C. Chuah, "Deep-Learning-Based Network Intrusion Detection for SCADA Systems," 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 2019, pp. 1-7, http://dx.doi.org/10.1109/CNS.2019.8802785 .

[11]. Ravi, Vinayakumar&Kp, Soman & Poornachandran, Prabaharan, Evaluation of Recurrent Neural Network and its Variants for Intrusion Detection System (IDS). International Journal of Information System Modeling and Design,43-63,2017, http://dx.doi.org/10.4018/IJISMD.2017070103 .

[12]. Ashfaq Khan, Muhammad & Kim, Yangwoo. Deep Learning-Based Hybrid Intelligent Intrusion Detection System, 2021, http://dx.doi.org/10.32604/cmc.2021.015647 .

[13]. C. Yin, Y. Zhu, J. Fei and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," in IEEE Access, vol. 5, pp. 21954-21961, 2017, http://dx.doi.org/10.1109/ACCESS.2017.2762418 .

[14]. A. H. Halbouni, T. S. Gunawan, M. Halbouni, F. A. A. Assaig, M. R. Effendi and N. Ismail, "CNN-IDS: Convolutional Neural Network for Network Intrusion Detection System," 2022 8th International Conference on Wireless and Telematics (ICWT), Yogyakarta, Indonesia, 2022, pp. 1-4, http://dx.doi.org/10.1109/ICWT55831.2022.9935478 .

[15]. Laghrissi, F., Douzi, S., Douzi, K. et al. Intrusion detection systems using long short-term memory (LSTM). J Big Data 8, 65 (2021). https://doi.org/10.1186/s40537-021-00448-4 .

[16]. Lirim Ashiku, Cihan Dagli, Network Intrusion Detection System using Deep Learning, Procedia Computer Science, Volume 185, 2021, Pages 239-247, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.05.025 .

[17]. J. Esmaily, R. Moradinezhad and J. Ghasemi, "Intrusion detection system based on Multi-Layer Perceptron Neural Networks and Decision Tree," 7th Conference on Information and Knowledge Technology (IKT), Urmia, Iran, 2015, pp. 1-5, https://doi.org/10.1109/IKT.2015.7288736 .

[18]. Supriya Shende, Samrat Thorat, 2020, Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security, International Journal of Engineering Research & Technology (IJERT) Volume 09, 2020, https://doi.org/10.17577/IJERTV9IS061016 .

[19]. V. K. Navya, J. Adithi, D. Rudrawal, H. Tailor and N. James, "Intrusion Detection System using Deep Neural Networks (DNN)," International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1-6, https://doi.org/10.1109/ICAECA52838.2021.9675513 .

[20]. Deore, B., Bhosale, S. Intrusion Detection System Based on RNN Classifier for Feature Reduction. SN COMPUT. SCI. 3, 114 (2022). https://doi.org/10.1007/s42979-021-00991-0 .